

EXHIBIT 69

1 Page 1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,

Plaintiffs,

vs. CIVIL ACTION FILE
NO. 1:17-CV-2989-AT

BRAD RAFFENSPERGER, ET AL.,

Defendants.

REMOTE VIDEOTAPED ZOOM DEPOSITION OF
DAVID HAMILTON

January 18, 2022
10:06 A.M.

Lee Ann Barnes, CCR-1852B, RPR, CRR, CRC

1 identification.)

2 THE WITNESS: Oops, it logged me out.

3 Hang on a second.

4 BY MS. KAISER:

5 Q. Sure.

6 A. Crap. I'm looking at the wheel. Hang on.
7 It's thinking.

8 Okay. Number 2.

9 Q. Do you recognize this document,
10 Mr. Hamilton?

11 A. Uh-huh. Yes.

12 Q. Is this a copy of your profile from
13 LinkedIn?

14 A. Looks like it.

15 Q. And is this something that you update
16 regularly?

17 A. I haven't in a while. Since -- since I
18 landed at -- at Shepherd, there's not much point in
19 it.

20 Q. Okay. And that was -- when did you begin
21 with Shepherd?

22 A. June, right as I left TrustPoint.

23 Q. In 2021?

24 A. Yes, ma'am.

25 Q. On -- at the bottom of page 1 of this

1 document, it indicates that you worked for
2 TrustPoint Solutions from October 2013 to June 2021;
3 is that correct?

4 A. It is.

5 Q. And what is TrustPoint Solutions?

6 A. They're a provider of security and
7 infrastructure services predominantly in healthcare.
8 They have some business outside in the public
9 sector.

10 Q. Sorry. I think you mentioned this, but
11 during the time that you had the title of chief
12 information security officer for the Georgia
13 Secretary of State's office, were you employed by
14 TrustPoint Solutions?

15 A. Yes, ma'am.

16 Q. So did you do work for the Secretary of
17 State's office on a contract basis?

18 A. No, not directly. Always through
19 TrustPoint.

20 Q. So you mean you, yourself, were not under
21 contract; the company --

22 A. Correct.

23 Q. -- TrustPoint was?

24 A. Correct.

25 Q. How much time did you spend per month on

1 work at the Secretary of State's office, roughly?

2 A. I guess it averaged out to be probably
3 half-time. There was some spikes there where it was
4 more full time as things ramped up for events such
5 as elections and things, incorporations. End of
6 year was a pretty busy time for the corporation
7 side. But as you look across, I would imagine it
8 would compute to be about half-time.

9 There were some times where I didn't --
10 wasn't there at all during a week because I was at a
11 different client.

12 Q. When you say "there at all," were you
13 physically at the Secretary of State's office?

14 A. Yes, ma'am.

15 Q. And when did you begin working for the
16 Georgia Secretary of State's office?

17 A. Summer of 2018. That's when the
18 engagement first began.

19 Q. And so from roughly summer of 2018 until
20 June of 2021, you spent approximately half your time
21 working on security issues for the Georgia Secretary
22 of State's office; is that correct?

23 A. Yes, ma'am.

24 Q. And what were your responsibilities for
25 the Georgia Secretary of State's office?

1 A. Just overseeing the -- the corporate
2 information security program, which included the --
3 the election side as far -- insofar as it -- the
4 registration side of the house. Not the Dominion
5 side, but the -- the corporation side of the house,
6 which is where you get a business license in
7 Georgia, and then also the Bureau of Licensing,
8 which is all the professional boards, the nursing
9 board and the barbershop folks and all those folks.
10 It's where you kind of go for -- that was the only
11 place that had PHI, so -- protected health
12 information.

13 Q. Understood. Okay.

14 And when you said -- you said that that
15 encompassed the election side insofar as the
16 registration side of the house.

17 Can you explain what you mean by that?

18 A. Well, there's -- there was a couple of
19 different buckets, right? The -- the main
20 things that I was concerned with is the -- is the
21 voter registration, the MVP site; security of the --
22 more or less the public-facing sites that managed
23 the registration of a voter.

24 Didn't have anything to do with the
25 tabulation of votes or the voting machines

1 themselves. All that was handled by the vendor.

2 Q. Interesting. Okay.

3 Who did you report to at the Secretary of
4 State's office?

5 A. Mr. Beaver. Merritt Beaver, the CIO.

6 Q. And did anybody report to you?

7 A. Yes. There was -- we had a couple of --
8 three. At one point there was one, then it got back
9 up to three when we restaffed. There were several
10 names in there. Do you want me to try to recall
11 them?

12 Q. Yes, if you can.

13 A. Okay. When I got there, it was -- I just
14 can't recall his name. Heavyset fella. I can't --
15 probably have to go to LinkedIn to figure that one
16 out. I can't recall his name.

17 When I left --

18 Q. Do you recall -- I'm sorry. Please
19 finish.

20 A. I was just going to say when I left, I can
21 tell you who those folks were.

22 Ronnell Spearman, who is -- who I think is
23 still there; Kevin Fitts; and then there was one
24 person that hired just as I was leaving. I actually
25 never got to meet him in person and I can't recall

1 A. I -- I didn't spend an awful lot of time
2 reading them. We just kind of glazed over them.

3 But, no, I -- I felt pretty good about my
4 memory about things, what happened. So...

5 Q. Did you ever recommend to the Secretary of
6 State at any point that they should have a full-time
7 chief information security officer?

8 A. Yes.

9 Q. Do you recall approximately when you made
10 that recommendation?

11 A. I think, basically, when -- when James
12 Oliver -- he was my predecessor. He was a full-time
13 employee.

14 I think initially when we came in, you
15 know, our edict was to kind of coach him up and get
16 him, you know, kind of more out there.

17 And James, very nice man, but he was kind
18 of reserved and quiet, and it's kind of hard to do
19 this job when you seal yourself in your office. You
20 kind of have to be out there and evangelize security
21 and get people excited about it, and he just didn't
22 have that gene.

23 So I -- you know, when the Secretary of
24 State made the decision to part ways with James, I
25 really thought the next step was for me to help the

1 Secretary of State find another full-time employee.

2 In the end, it wasn't. What they decided
3 to do is do a fractional kind of a situation where
4 they'd continue that relationship and kind of let me
5 sit in the chair.

14 Q. And I believe you said that you didn't --
15 you personally didn't have a budget.

16 Did you ever make a recommendation that
17 the chief information security officer should have a
18 budget?

19 A. No. I mean, they -- they had a budget for
20 security; it's just I wasn't -- I didn't have any
21 signing authority. I couldn't go spend money. You
22 know, I didn't have an expense account or anything
23 like that.

24 Anything I wanted to spend money on, I had
25 to go to -- go to Merritt for, and he worked it out

1 BY MS. KAISER:

2 Q. Did you have any --

3 A. -- the wrong place to put it.

4 Q. Did you have any involvement with making
5 that transition of the Kennesaw server?

6 A. No, ma'am. No, ma'am. That was way
7 prior. 2016, I guess. So...

8 Q. We've mentioned Fortalice several times
9 now.

10 Are you aware that Fortalice conducted a
11 series of cyber risk assessments for the Secretary
12 of State's office in 2017 and 2018?

13 A. Yes, I -- I have knowledge of those.

14 Q. What role, if any, did you have in working
15 with Fortalice on those cyber risk assessments?

16 A. The second one in 2018, I believe that was
17 during my tenure, at least I got the report. The
18 2017, I think they just passed it to me as history.
19 So...

20 Q. And can you tell me, in general terms,
21 what Fortalice found in its 2017 and 2018 cyber risk
22 assessments for the Secretary of State's office?

23 A. There was a number of items. They
24 classified them as high, medium, low, based on their
25 experience, and then gave us an opportunity to

Page 46

1 either accept or -- or deny, you know, what was
2 going on.

3 It gives us a good basis for kind of
4 reprioritizing our work within the State to figure
5 out where we should spend our money and time trying
6 to go after the things that are the most vulnerable.
7 It's a judgment call.

8 MS. KAISER: Can you pull up Tab 3,
9 please.

10 (Plaintiffs' Exhibit 4 was marked for
11 identification.)

12 THE WITNESS: Is there another document?
13 I'm sorry.

14 BY MS. KAISER:

15 Q. It's being loaded right now.

16 A. Okay. I'm sorry.

17 Q. It takes a minute with larger documents,
18 so apologies --

19 A. Gotcha.

20 Q. -- for the delay.

21 A. Okay. Exhibit B. Okay.

22 Q. So if you scroll down to the next page,
23 you'll see this is the cover page of the report.

24 Do you recognize this as the 20- --

25 November 2018 report that Fortalice provided to the

1 Secretary of State's office?

2 A. I think so. Let me go down to the meat of
3 it here. Hang on.

4 MR. MILLER: Mary, this is another sealed
5 document. I can't recall from the 2019 hearing
6 if we -- how we designated this.

14 MS. MARKS: Sure, I will. And if you will
15 let me know when I can safely come back on.

16 Thank you.

17 (Ms. Marks left the Zoom deposition.)

18 BY MS. KAISER:

19 Q. Mr. Hamilton, have you had a chance to
20 take a look at the document now?

21 A. I have, yep.

22 Q. And do you recognize this as Fortalice's
23 2018 Red Team Penetration Test and Cyber Risk
24 Assessment?

25 A. I do, yep.

Page 48

1 Q. If you could turn to page 8 of the report.

2 A. Okay.

3 Q. The top section there says " [REDACTED]

[REDACTED] "

5 Do you see that?

6 A. Correct.

7 Q. That next paragraph reads, " [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] "

11 A. Right.

12 Q. If you skip one sentence, it says, " [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] "

17 Do you see that?

18 A. I do.

19 Q. So do you understand this section of the
20 report to address progress made on the top ten risks
21 identified by Fortalice in 2017?

22 A. Uh-huh. Yes.

23 Q. Do you know why three of those top ten
24 risks were not tested in 2018?

25 A. I do not. Usually, it's a -- when a --

1 when a security firm does a -- a pen test or a
2 security assessment, they use last year and the
3 current year to show progress or show kind of a
4 trend, are you getting better or are you getting
5 worse. So usually you test the same things.

6 The only reason I would think that we
7 missed is if they were specifically taken out of
8 scope.

9 Q. Okay. And this report says that of the
10 top ten risks identified in 2017, only three had
11 been remediated in 2018; is that correct?

12 A. That's what this states, correct.

13 Q. If you can flip to page 5 of the report.

14 A. Okay. Hang on. It's back. Hang on.

15 Okie-doke. I'm here.

16 Q. The second paragraph on page 5, it reads,

17 " [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] . "

22 Do you see that?

23 A. Right.

24 Q. And that first bullet point reads, " [REDACTED]
[REDACTED] . . . "

1 Do you see that?

2 A. I do.

3 Q. And are those recommendations detailed on
4 pages 6 and 7 of the report --

5 A. I believe so.

6 Q. -- in this table?

7 A. Yeah.

8 Q. What steps did the Georgia Secretary of
9 State's office take to implement these 20
10 recommendations from Fortalice?

11 A. I can't speak to the first half of that
12 year because I wasn't there, but it might have had
13 something to do with -- and this is a little bit of
14 speculation on my part -- is that that might have
15 been the reason for our involvement, is that Merritt
16 didn't feel like things were moving along fast
17 enough.

18 So he wanted -- that was one of the things
19 that we were to come in and coach up for James
20 Oliver is to kind of get him excited about this
21 stuff and get moving on some of these things that
22 were identified.

23 And I think this was the list that I gave
24 the status on I guess about halfway through the
25 tenure. That was one of the exhibits or the

1 statements that I made to the Court.

2 So I don't know what the status is now, of
3 course, because I've been gone six months, but they
4 were well on their way to taking care of those
5 and -- and others that were found along the way.

6 So...

7 Security is -- itself truly is a -- it's a
8 journey; it's not a destination. You're never done.
9 I mean, there's always -- the threat landscape
10 changes every day. Things change every day.

11 So, you know, it's a snapshot in time. At
12 the time that Fortalice did this, this is what they
13 found. They could have waited three weeks and did
14 another one and found something else and not found
15 three others. So it's just a snapshot in time.

16 Q. Sure.

17 At the bottom of page 5 of the report, the
18 last paragraph there, it says, " [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]."

23 Do you see that?

24 A. I do.

25 Q. To your knowledge, did the Secretary of

1 State's office dedicate any additional resources to
2 addressing the security risks Fortalice identified?

3 MR. MILLER: Objection. Lack of
4 foundation.

5 THE WITNESS: I believe I was one of those
6 resources.

7 BY MS. KAISER:

8 Q. Do you have any awareness of whether
9 internally at the Secretary of State's office, any
10 additional resources were applied to addressing
11 these security risks?

12 A. Yeah, when -- I was able to recall that
13 gentleman's name, Adam Abell. He -- he was the one
14 that was working with James on a day-to-day basis.
15 So it was only the two of them.

16 Shortly after my arrival, they moved
17 Ronnell Spearman over from the services side of the
18 house and opened up a req for adding another party
19 to the security. I think all of that was based on
20 the findings.

21 So most of the time that I was there, we
22 were at a staff of three and -- not including me,
23 except when we ended up letting one guy go and that
24 gap of time when we were looking for the next
25 person.

1 MS. KAISER: Will you add Tab 4, please,
2 Zach.

3 BY MS. KAISER:

4 Q. We're going to bring up the next exhibit,
5 Mr. Hamilton.

6 A. Okay.

7 (Plaintiffs' Exhibit 5 was marked for
8 identification.)

9 BY MS. KAISER:

10 Q. If you scroll down to the second page, I
11 believe you -- you stated that you -- you know, you
12 made a statement in this case.

13 Do you recognize this to be the
14 declaration that you provided in this case?

15 A. Yes, ma'am. One of two, correct.

16 Q. Correct.

17 Let's see. This one is dated August --
18 August 25, 2020.

19 Do you see that?

20 A. That sounds about right, yep.

21 Q. Okay. Did you draft this document, sir?

22 A. I did.

23 Q. And the purpose of your declaration, as
24 you mentioned, was to go through the recommendations
25 from Fortalice and give a status update on how they

1 were being resolved or remediated; is that right?

2 A. Correct.

3 Q. I just want to walk through a couple of
4 these.

5 So Number 2, the "Two-Factor
6 Authentication," do you see that?

7 A. Uh-huh.

8 Q. It says the "Status" was "Accepted and
9 Partially Remediated."

10 A. Uh-huh.

11 Q. Do you see that?

```
12             All right.  And Number 5 was "Non-Unique  
13 Local Admin Passwords."
```

14 Do you see that?

15 A. I do.

16 Q. The "Status" was "Accepted and
17 Compensating Control Applied."

18 Do you see that?

19 A. Correct.

20 Q. What did you mean by "compensating control
21 applied"?

22 A. The long-term solution would be to go to a
23 PAM, which is a privileged account management
24 solution, but that's a pretty heavy lift
25 financially.

1 So in the short term, what we did is apply
2 the out-of-the-box LAP Solution that allows the --
3 the encryption of the endpoints.

4 And also we put in some policy and
5 procedures that when the guys were out working on
6 people's machines, that they -- they have to go to a
7 centralized password vault to be able to access
8 them.

9 They -- in the past, they had the same
10 administrative password on all the systems to make
11 it easy to maintain, you know, your IT help desk
12 guys. But it was a problem for me because I -- I
13 knew that, you know, there was some churn in that,
14 and it's just not a best practice. You should have
15 a unique admin password on every endpoint.

16 Q. Number 10 is "Lack of Security Controls
17 for PCC."

18 You see that?

19 A. Right.

20 Q. And the "Status" for that is "Accepted and
21 Remediation On-Going."

22 A. Yeah. I -- I -- during my tenure there at
23 the State, I think that was the most difficult
24 vendor to deal with, the PCC folks, because they
25 would say one thing and do another.

1 And I even got to the point where I sent
2 them an attestation of a -- basically, a list of
3 minimum security. I just wanted somebody to sign
4 their name to the fact that, you know, some -- the
5 minimum is being done. And they signed it, but in
6 my heart of hearts, I kind of knew that they
7 probably weren't doing it.

8 So -- but at that point, they had already
9 made the decision to remove PCC and move to another
10 vendor, so it would have been kind of wasted breath
11 at that point. Which was, I -- I think, a good -- a
12 good decision to move away from PCC. They just --
13 they just weren't the right guys. That's all.

14 Q. And we'll come back to PCC later on
15 today --

16 A. Okay. Okay.

17 Q. -- but just quickly, what did they have
18 responsibility for with respect to the election
19 system?

20 A. The coding, the actual coding of the
21 program itself. The Secretary of State didn't
22 employ anybody that -- that actually wrote computer
23 code, that developed applications. They -- they
24 always relied on third-party vendors for that.

25 And they did the ENET system and they did,

1 you know, the corporation side and -- and also some
2 of the licensing sites as well. They were kind of
3 the go-to company for all things Secretary of State.

4 I think prior to my arrival, the word
5 was -- is they were a lot better back then. But
6 they had some changes. A lot of people left, good
7 people left, that kind of thing, and over time it
8 just became a problem. So...

9 Q. A problem from a security perspective, was
10 that your view?

11 A. Yeah. Even -- yeah, even the stability of
12 the code line, I think, was wearing very, very thin
13 on the customer, being the Secretary of State. They
14 were getting tired of, you know, things that -- you
15 had mentioned before the confidential --
16 confidentiality, integrity, and availability. That
17 availability part of that triad is pretty important
18 when it comes to the Secretary of State. They
19 always want to be available because they don't want
20 to be viewed as, you know, not on the -- not on the
21 ball.

22 So -- and there were some availability
23 problems with PCC. Some of their practices were not
24 best -- best practice. And they would fix things on
25 the fly and although it fixed it at the moment, they

1 wouldn't move that fix back into the code line, so
2 the very next time they did a revision, they would
3 re-break the thing.

4 And that is kind of a, you know, 101
5 change control operation. Somebody wasn't watching
6 the store. So...

7 And we tried to help grow them. You know,
8 we gave them a lot of feedback, probably a lot more
9 than they ever wanted.

10 And then they were purchased by another
11 firm, and that gentleman -- they had a CISO there.
12 He's the gentleman that actually attested to the
13 fact that their minimum security met the minimum
14 based on what I had sent them. I think he was
15 hopeful that it would get that way, but I had my --
16 like I said, I had my doubts, so to speak.

17 Q. All right. Well, going back to your
18 declaration, Mr. Hamilton, we can -- we can keep
19 walking through them one by one, but by my count,
20 there were 11 out of 20 recommendations that,
21 according to your declaration, had not been fully
22 remediated.

23 A. Right.

24 Q. Does that sound about right?

25 A. (Nodded head.)

1 Q. Okay. And that was the status as of
2 August 2020; correct?

3 A. Correct, so basically three months into my
4 tenure. That's about right, yeah.

5 Q. Three months into your tenure. Okay.

6 And -- but that was nearly two years after
7 Fortalice issued their cyber risk assessment in
8 November 2018; is that correct?

9 A. Correct.

10 MR. MILLER: Objection. Lack of
11 foundation.

12 BY MS. KAISER:

13 Q. And so nearly two years after Fortalice
14 issued that report, at least half of their
15 recommendations had not been fully implemented; is
16 that correct?

17 MR. MILLER: Objection. Asked and
18 answered.

19 THE WITNESS: It sounds like it, yeah.

20 BY MS. KAISER:

21 Q. Based on your experience and training,
22 does it seem reasonable to have a cybersecurity
23 vendor identify security risks in your system and
24 then not take recommended steps to address those
25 risks for nearly two years?

1 MR. MILLER: Objection to form. Lack of
2 foundation. Calls for speculation.

3 THE WITNESS: In -- in my professional
4 opinion, it's not uncommon. Some of -- some of
5 the things that we're faced with have budgetary
6 constraints.

7 The bottom line is we present -- as
8 security people, we present to the business and
9 say, "Here's the nine things we've got to do.
10 You know, what's our bucket of money look like?
11 What does it take, you know, horsepower,
12 people, whatever?" And then the business makes
13 the decision finally on -- on what -- what to
14 focus on. We make recommendations and then we
15 move on those.

16 But we made pretty good headway, I
17 think --

18 BY MS. KAISER:

19 Q. Were you pushing the Secretary of
20 State's --

21 A. -- before I left. So...

22 Q. Were you pushing the Secretary of State's
23 office to move faster or make more headway on these
24 recommendations from Fortalice?

25 A. Yes, ma'am. I was kind of the evangelist,

1 and, yeah, I was -- I was not shy about it. So...

2 Q. Why were you pushing that?

3 A. Just to get -- get moving, right? We had
4 the time and some of the things, like was outlined,
5 are low cost or no cost. It doesn't mean that it --
6 I mean, no cost is nobody has to write a check to a
7 vendor.

8 But the big thing is -- is the headcount.

9 It's the talent that you have in-house that are able
10 to do these tasks. And a lot of my time there
11 was -- was training, mentoring, kind of teaching
12 people how to kind of ramp things up. So -- yep.

13 Q. Have you -- you felt that these
14 recommendations from Fortalice were good ones,
15 correct, that would improve the security of the
16 system?

17 A. Yeah. That's why on -- on the -- on the
18 statement where I said "Accepted" -- in any -- in
19 any situation where a -- a security firm comes in
20 and does an assessment or a pen test and they
21 present you with the findings, you're able to accept
22 those or not accept them.

23 An example of not accepting is either it
24 was out of scope or something that had long been
25 fixed and they missed it. You know, things like

1 that.

2 So in most of these cases, I believe I
3 accepted most of these because I verified that they
4 were still valid.

5 Q. Has Fortalice done any additional work for
6 the Secretary of State's office since the
7 penetration testing in 2018?

8 A. I -- I -- they had an annual -- they had
9 an annual test and assessment, a pen test.

10 Q. And when you say "pen test" --

11 A. I know we --

12 Q. -- is that --

13 A. Penetration test. That's somebody from
14 the outside tries to get in. There's three forms of
15 that. There's, you know, the white hat, the black
16 hat, and the gray hat.

17 So this was very much -- we did not give
18 them the keys to the castle. We wanted them to
19 replicate the outside world, so that becomes a black
20 hat operation.

21 Gray hat is when you give them a little
22 bit of a path, you know a little bit about the
23 environment.

24 And then white hat, of course, is you give
25 them carte blanche to the environment and then they

1 just go -- usually that's an internal pen test.

2 But all of these were external.

3 Q. And to your understanding, Fortalice did
4 one of these pen test assessments each year since --

5 A. Yes, ma'am.

6 Q. -- 2018?

7 And did they test the -- the entire part
8 of the Secretary of State's network or -- or
9 portions of it in those years, do you know?

10 A. Most of it was just the business network,
11 right? It was the business network and the
12 public-facing websites, nothing specific to --

13 You know, every business has a certain
14 number of IP addresses that face the public, and I
15 think in previous years, because of cost, they had
16 kind of truncated that list a little bit. Because
17 they do charge per IP address.

18 And I know one of the years that I was
19 there, I went ahead and had them test everything,
20 every public IP address that we had. It was
21 expensive to do, but you -- you kind of want a basis
22 to kind of run from. So...

23 Q. Did these pen -- penetration tests include
24 the portions of the election system that the
25 Secretary of State is responsible for?

1 A. Yes, ma'am. The registration side, yes.

2 Q. Did you personally work with Fortalice on
3 these penetration tests?

4 A. No. I -- I'm just the client. They're
5 done in a vacuum and then they report back in a
6 draft mode and we talk about them, and then they
7 make a final report.

8 Q. Did they provide those reports to --

9 A. To Merritt, yeah. Again --

10 Q. Did you review --

11 A. -- that was done because they were the
12 customer.

13 Q. Correct.

14 But did you review those reports?

15 A. I did.

16 Q. And you said that there were discussions
17 of the reports.

18 Were you involved in the discussions?

19 A. I would say most of them, but maybe not
20 all of them.

21 Q. So to your knowledge, Fortalice conducted
22 and provided a report regarding a penetration test
23 in 2019; is that correct?

24 A. I would think so, yes.

25 Q. And in 2020?

1 MR. MILLER: Objection. Lack of
2 foundation.

3 | BY MS. KAISER:

4 Q. Let's see. If you move forward on this
5 document to the February 26, 2021, entry.

6 A. Okay.

7 Q. It's on the page ending in -2785.

8 A. -2785. Okay. I got it.

9 Q. The last bullet there says, "Weekly
10 update." It says, "vCISO services have been
11 mentioned."

12 A. Right.

13 Q. "Kyle and Paul are setting up meeting to
14 discuss with Dave Hamilton to get them caught up on
15 a backlog of security tasks."

16 Do you --

17 A. Right.

18 Q. -- see that?

19 A. Right.

20 Q. Do you know what that is referring to?

21 A. Yeah. I had mentioned to Fortalice that I
22 was planning on leaving the State as soon as I found
23 another position and that they needed to -- you
24 know, as the other partner, if they had the ability
25 to step in.

1 You know, I wanted to take care of the
2 State. TrustPoint did not have any resources they
3 had left, so there wasn't anybody from our firm.
4 And I checked it out with my boss and he said it
5 would be fine to kick it to them and say, "Listen,
6 you know, we want to take care of our customer and
7 if you're getting ready to leave, then, you know,
8 you need to give it to them."

9 They subsequently decided that they
10 couldn't fill that seat because of a conflict of
11 interest.

12 Q. What was the backlog of security tasks
13 that are --

14 A. I think --

15 Q. -- mentioned here?

16 A. I think I pitched to them that there was
17 definitely work to be done, it was a work in
18 progress, and it wasn't going to be -- I think my
19 emphasis there was for -- for them to please be
20 interested, you know.

21 Because they would want to bill,
22 obviously. They didn't want to just come in and be
23 a -- more of a maintainer than a fixer, right? So
24 my emphasis there was just to kind of get them
25 interested in coming in and stepping in for me.

1 Q. In your view, why was there a backlog of
2 security tasks?

3 A. Well, I think it was just, you know, we
4 needed some help. You know, we had some staff
5 turnover and some people leave and I was getting
6 spread pretty thin between there and Imperial and I
7 wasn't there every week, and I just felt like I
8 needed to kind of get people interested in coming to
9 help.

10 Q. If you move forward in the document to the
11 entry for April 16, 2023 [sic], it's on the page
12 ending in -2784.

13 A. -2784. Okay. April 16 you said?

14 Q. 16, yes.

15 A. Yes, ma'am. Got it.

16 Q. It says "Project Status," and the second
17 bullet point there says, "Pen test wrapping up."

18 Do you see that?

19 A. Okay. Adam Brown. Okay.

20 Yeah, I worked with --

21 Q. Does that suggest --

22 A. -- Adam.

23 Q. Does that suggest to you that Fortalice
24 did conduct penetration testing in 12 --

25 A. Sounds like it, yeah.

1 if you insist, then let the games begin. Fair
2 warning."

3 Do you see that?

4 A. Yep.

5 Q. And it looks like -- it looks like this
6 was sent to soscontact@sos.ga.gov?

7 A. Right. That's just the -- the basic
8 website. It's like sending a note to the webmaster,
9 right.

10 Q. Okay. And then this was forwarded on to a
11 group of people, including -- let's see -- including
12 Chris Harvey and Kevin Rayburn.

13 Do you see that?

14 A. Yep. James Oliver. Right.

15 Q. Right.

16 But you don't recall -- you don't have any
17 recollection of this email or this incident?

18 A. No, ma'am.

19 Q. And you don't recall any similar threats
20 during your time at the Secretary of State's office?

21 A. No, nothing like that. It's been my
22 experience that people who threaten usually don't do
23 it. It's the people that don't say anything that do
24 things like this.

25 Q. Do you know whether there has ever been a

1 cybersecurity assessment done of Georgia's voting
2 equipment?

3 A. I do not. As I understood it, that was
4 the privy of the Dominion folks and that they were
5 independently certified. I don't know much about
6 that process.

7 Q. So you're not aware of any cyber
8 assess- -- cybersecurity assessment of the voting
9 machines?

10 A. No, ma'am.

11 Q. Are you aware of any reports or
12 conclusions regarding any security vulnerabilities
13 with the BMD system?

14 A. Not -- not specifically, because it kind
15 of fell outside my scope. So...

16 Q. Are you generally aware of any?

17 A. No, I -- I can't recall any that -- I
18 mean, there was always the underpinnings of somebody
19 trying to do something, but we live with that every
20 day. So...

21 Q. So you're not personally aware of any
22 security breaches or vulnerabilities involving the
23 BMD system.

24 MR. MILLER: Objection. Asked and
25 answered. Lack of foundation.

3 | BY MS. KAISER:

4 Q. Are you aware of any complaints regarding
5 the security of the BMD system?

6 A. No. I -- I think I read some news stories
7 and things like that, but nothing specific.

Q. What is the Election Center?

9 A. I think that's the hardened facility that
10 they moved to. I've never been in it. Not meaning
11 like moved the servers to. I think that was like
12 the -- the war room, so to speak. It's where the
13 people went during an election.

14 Q. The people but not the servers, you said?

15 A. No. Servers are maintained in -- in
16 secure data centers.

17 Q. Okay. What server is the election
18 management system for the new BMD election system,
19 where is that currently hosted?

20 MR. MILLER: Objection. Foundation.

1 reason people patch is because they're afraid of the
2 Internet. It's not on the Internet; we don't need a
3 patch.

4 That's not necessarily the way I think,
5 so -- you still gotta be current for the support
6 reasons.

7 Q. So why did you include a frowny face after
8 that comment?

9 A. Just -- it's kind of -- for me, when I see
10 a frowny face, it's to kind of remind me that that
11 was a bad thing. Just a note-taking style.

12 Q. So that was something that you thought
13 needed to be changed?

14 A. Yes.

15 Q. Two bullets down from that, it says, "Need
16 to be able to scan every USB attached storage device
17 connected to prior [sic] use. Cannot ensure USB is
18 free from malware, keylogging, etc."

19 Do you see that?

20 A. Yes.

21 Q. What did you mean by that comment?

22 A. So it was common practice for the -- for
23 the data to be shared with the counties once they
24 drafted or came up with a -- a strawman of what
25 their ballot looks like. They would share that data

1 via USB. They would, you know, FedEx it to them and
2 then they'd -- they'd mark up changes and then
3 they'd FedEx the USB key back.

4 Even though Michael had an internal
5 process that when he started the event, he would
6 take a USB drive out of the package and start, he --
7 he thought that was good enough and -- because he
8 encrypted it and did a lot of other things.

9 But, you know, I had a different
10 experience in life, so I decided that I thought that
11 he needed to go to a more secure managed solution
12 for USB drives, and I proposed moving to a -- an
13 actual managed USB key program.

14 And I'm not sure if that ever got funded
15 or not. It was not an insignificant amount of
16 money, but I think they decided that the -- you
17 know, the juice wasn't worth the squeeze, so to
18 speak.

19 Q. So to -- to your knowledge, at the time
20 you left the Secretary of State's office, that
21 recommendation had not been implemented --

22 A. No. They had -- they had quotes -- we had
23 quotes and we actually had sample units that Michael
24 Barnes had where he was using it for his work flow
25 to see how it moved.

1 But I think I left before that decision
2 was made. So...

3 Q. And why did you make that recommendation?

4 A. Because he was using commodity-based USB
5 drives.

6 Q. And why was that not a best practice, in
7 your view?

8 A. Because they're not made in the U.S.

9 They're -- they could have all kinds of things on
10 them. We don't know.

11 The only way to really make sure is to,
12 you know, wipe the thing free of -- it has to go
13 through a process of sanitization before you use it.

14 And, you know, I just -- I really like the
15 idea of a managed USB. The name of it is called
16 DataLocker, and -- and it actually has code on it
17 that you're able to track, much like a LoJack, and
18 it keeps a log of every file ever written and a
19 log -- a file of every -- every time it's read,
20 every time it's loaded, every time anything happens
21 to it, and it uploads it to a cloud-based service so
22 you can see where these drives are; and if someone
23 got ahold of one of these drives and put it in a USB
24 slot that wasn't authorized, that it would wipe the
25 contents securely and -- kind of like brickling a Mac

1 if you don't -- if you're not the owner kind of
2 deal.

3 But it was a pretty significant outlay of
4 cash to get that done. And I think he liked the
5 idea. I think -- he wasn't as paranoid as I was.
6 Michael Barnes. Sorry. Didn't mean to say "he."

7 MS. KAISER: Can you add Exhibit 12,
8 please -- Tab 12?

9 THE WITNESS: 14.

10 (Plaintiffs' Exhibit 14 was marked for
11 identification.)

12 BY MS. KAISER:

13 Q. If you look at the first email in this
14 chain, it's from Michael Smith at DataLocker.

15 Do you see that?

16 A. Yeah, all the way at the bottom? Got it.
17 Okay.

18 Q. Is this the vendor that you were just
19 discussing?

20 A. Yes, ma'am.

21 Q. So it looks like in July of 2020, you
22 reached out to DataLocker and they sent you a
23 response.

24 A. Correct.

25 Q. And then your email at the top of

1 BY MS. KAISER:

2 Q. This is --

3 A. Okay.

4 Q. This is a report from Fortalice Solutions.

5 Do you see that?

6 A. Yes.

7 Q. Dated July 14, 2020?

8 A. Right.

9 Q. If you look at page 2 of the report --
10 it's the third page of the document, but it says
11 page 2 at the bottom --

12 A. Okay.

13 Q. -- under Section 1.1, "Overview," it says,
14 "In June of 2020, Secretary of State Georgia
15 received report of two vulnerabilities in a web
16 application hosted at
17 [https://www\[.\]mvp\[.\]sos\[.\]ga\[.\]gov](https://www[.]mvp[.]sos[.]ga[.]gov)."

18 Do you see that?

19 A. Correct. Yep.

20 Q. All right. So this is -- the "MVP" is the
21 My Voter Page; is that right?

22 A. Yes.

23 Q. And the next sentence says, "Upon
24 attempted remediation, SoSGA requested that
25 Fortalice validate the remediation attempts."

1 Do you see that?

2 A. I do.

3 Q. Do you recall anything about this
4 incident, about --

5 A. Yeah. Basically --

6 (Cross-talk.)

7 A. Basically, we were asking Fortalice to
8 verify what we were being told by PCC as "it's
9 fixed." Because we didn't have the -- the
10 wherewithal to, you know, go through this stem by
11 stem, we got Fortalice to do it as a third -- third
12 party. So...

13 Q. And what did Fortalice find?

14 A. They found that actually they had not
15 remediated it sufficiently, and they made a
16 suggestion on how to fix it the right way. And we
17 fed that information back to PCC.

18 Q. This is in 2020; correct?

19 A. Probably. Yeah.

20 Q. Did PCC still have responsibility for the
21 MVP page in 2020?

22 A. No.

23 Q. So why did you need to feed the fix back
24 to PCC?

25 A. Because they still write the code. They

Page 161

1 still manage the application, they just don't manage
2 the hardware. So they're still responsible for the
3 code line.

4 Q. So when you identified a vulnerability on
5 the My Voter Page, you still had to rely on PCC to
6 fix it?

7 A. Correct.

8 Q. If you look at page 4 of the Fortalice
9 report --

10 A. Okay.

11 Q. -- under "Conclusion," it says, "The
12 remediation attempts that are currently in place
13 partially fix the issues in the original report, but
14 more work needs to be done to secure the website
15 from potential attacks."

16 Do you see that?

17 A. Right.

18 Q. "In addition to the checks performed,
19 Fortalice noticed other areas of potential impact
20 that, while unconfirmed, Fortalice believes could be
21 used to further exploit the site or the servers
22 hosting it. Fortalice recommends having the
23 application thoroughly reviewed for similar issues."

24 Do you see that?

25 A. Correct. Right.

1 Q. Do you know whether that recommendation
2 was accepted, to have the application reviewed for
3 similar issues?

4 A. I -- I didn't. I didn't have an
5 application-specific review done for them because
6 I -- I think at that point, the decision had been
7 made to jettison PCC.

8 So I think leadership looked at it as,
9 "We're going away from them, so, you know, we're
10 going to spend the time on the new stuff."

11 We did feed all this information back to
12 them, that there might be some other areas and, you
13 know, as a partner, we expect them to, you know,
14 find some of their own issues. We don't want to
15 be -- be their QA group. So...

16 Q. I just want to make sure I understand the
17 timing, because, you know, I -- I've understood you
18 to say that PCC was jettisoned in 2019; is that
19 right?

20 A. From the operational standpoint, right,
21 the care and feeding of the servers, the patching,
22 that kind of stuff, and the contract of housing the
23 servers and we're paying them to do that service.

24 But the actual code line, the development
25 and the -- and the -- you know, the changes that

1 were made to MVP and all those -- OLVR, all those
2 systems, were still under their control because they
3 were the developers.

4 Q. Right.

5 And so by 2020, the Secretary of State's
6 office had taken over with respect to the security
7 of these applications; is that right?

8 A. Well, insofar as we can handle it from
9 the -- from the edge. But as far as internal to the
10 actual application, we still have to rely on PCC to
11 do what they profess they're experts at.

12 So that's why we run these monthly checks,
13 and what we do with Fortalice with pen tests is to,
14 you know, trust but verify, right? We verify what
15 they told us to be true.

16 Because the Secretary of State doesn't
17 employ any developers, that's -- that's a bit of
18 a -- a hill to climb. We didn't have anybody in
19 there that wrote code, so we couldn't really
20 challenge them on a code line level. We just
21 identified, "Hey, this doesn't work right; go fix
22 it."

23 Q. So when --

24 A. This --

25 Q. -- Fortalice recommended -- recommended a

1 thorough application review, is that --

2 A. Uh-huh.

3 Q. -- something that the Secretary of State's
4 office could carry out, or would you have to rely on
5 PCC?

6 A. No, no, no. We would have to actually
7 hire another company to do that as a third party.

12 There's a term "OWASP." It's for the --
13 you know, the top 25 things that people do wrong in
14 programs. And they were missing some of the basic
15 stuff, so we started beating up on them about being
16 at least OWASP compliant.

17 But it would have been a third party. I'm
18 not sure if -- if Fortalice provided that. They --
19 they may or may not have had that as -- it sounds
20 like it is. It sounds like, "Oh, by the way, you
21 know, we could do this for you," cha-ching, you
22 know, that kind of thing.

23 Q. But to your knowledge, that kind of
24 thorough review of the application for similar
25 issues to the ones you identified at the time was

1 never done?

2 A. Not while I was there. It might have been
3 done after I left, but, again, that's --

4 Q. You're not aware of that?

5 A. I'm not aware of it, right.

6 MS. KAISER: Tab 18, please. I'm adding
7 Exhibit 20.

8 THE WITNESS: Okay.

9 (Plaintiffs' Exhibit 20 was marked for
10 identification.)

11 THE WITNESS: Okay.

12 BY MS. KAISER:

13 Q. This is an email from you dated April 29,
14 2021.

15 A. Right.

16 Q. Do you see that?

17 And it says to Ronnell Spearman, Derek
18 Hawkins, and DeVon King.

19 A. Right.

20 Q. And are those -- are those the three
21 security analysts that reported to you --

22 A. At that --

23 Q. -- at this time?

24 A. -- time, right.

25 COURT REPORTER: One at a time, please.

1 operational world of running a business, we have to
2 do these things and reprioritize.

3 So that's basically what that was.

4 Q. Do you understand that Dr. Halderman has
5 analyzed the voting equipment that is used in
6 Georgia today to assess the reliability and security
7 of that equipment?

8 A. I didn't know that he personally had done
9 it, no. I know --

10 Q. So you weren't aware that he's issued a
11 detailed report finding that the current system
12 suffers from many significant vulnerabilities?

13 A. I didn't --

14 MR. MILLER: Objection. Lack of
15 foundation.

16 THE WITNESS: Yeah, I -- I didn't. Sorry.
17 BY MS. KAISER:

18 Q. You didn't know -- you just didn't know
19 about that report one way or the other?

20 A. No. I'm not --

21 MR. MILLER: Objection.

22 THE WITNESS: -- in the academic world. I
23 don't spend a lot of time reading papers and
24 things like that. So...

1 BY MS. KAISER:

2 Q. I'm sorry. It was not a paper, but a
3 report in this case.

4 A. Yeah, that's fine.

5 MR. MILLER: Objection. Lack of
6 foundation.

7 BY MS. KAISER:

8 Q. So you were not -- not aware of it?

9 MR. MILLER: Same objection.

10 COURT REPORTER: The answer again, please?

11 THE WITNESS: No, I -- I was not aware of
12 it.

13 COURT REPORTER: Thank you.

14 BY MS. KAISER:

15 Q. Do you understand that the current BMD
16 voting system uses QR codes to tally votes?

17 A. I do --

18 MR. MILLER: Objection --

19 THE WITNESS: -- and only because I vote
20 in Georgia. I saw them. So...

21 COURT REPORTER: The objection again,
22 please?

23 MR. MILLER: Lack of foundation.

24 COURT REPORTER: Thank you.

25 Please -- please let him get in an

1 objection and her finish the question. Thank
2 you.

3 THE WITNESS: All right.

4 BY MS. KAISER:

5 Q. Are you aware that the current election
6 equipment can be hacked in a way that QR codes can
7 be changed so that they don't reflect what the voter
8 actually intended when they voted on the machine?

9 MR. MILLER: Objection. Lack of
10 foundation.

11 THE WITNESS: I did not.

12 BY MS. KAISER:

13 Q. Based on your experience and training, if
14 that were the case, would you take measures to
15 eliminate that vulnerability?

16 MR. MILLER: Objection. Lack of
17 foundation.

21 BY MS. KAISER:

22 O. Would it be a high priority on the list?

23 MR. MILLER: Same objection.

24 THE WITNESS: I -- again, it -- it all

25 depends on what else was going on at the time.

1 So . . .

2 BY MS. KAISER:

3 Q. A vulnerability that would allow a QR code
4 to be changed to change votes, would that be
5 considered high priority?

6 MR. MILLER: Objection. Lack of
7 foundation. Asked and answered.

12 So for them, I would imagine it would
13 cause some heartburn, but not -- I -- out of
14 scope for me.

15 BY MS. KAISER:

16 Q. Would it surprise you to learn that the
17 Secretary of State's office has taken no measures to
18 mitigate or eliminate any of the vulnerabilities
19 that Dr. Halderman has found with the existing
20 equipment in Georgia?

21 MR. MILLER: Objection. Lack of
22 foundation. Form of the compound question.
23 Misstates testimony.

1 his list was.

2 BY MS. KAISER:

3 Q. Based on your experience and training in
4 cybersecurity, if a cybersecurity expert identifies
5 vulnerabilities with a voting system, would you
6 think it would be a high priority to address those
7 vulnerabilities?

8 MR. MILLER: Objection. Lack of
9 foundation. Calls for speculation.

10 THE WITNESS: Yeah, I don't -- I would
11 be -- I'd be suspect of it. Just -- I'd want
12 to look at it myself.

13 BY MS. KAISER:

14 Q. Would you look at it yourself, though?

15 MR. MILLER: Same objection.

16 THE WITNESS: If given the opportunity, I
17 guess, yeah.

18 BY MS. KAISER:

19 Q. And if you, yourself, identified security
20 vulnerabilities, would it be a high priority --
21 priority to fix those vulnerabilities?

22 MR. MILLER: Objection. Lack of
23 foundation. Calls for speculation.

24 THE WITNESS: All depends on the -- the
25 judgment at the time, I guess, of what's going

1 on.

2 BY MS. KAISER:

3 Q. If you had responsibility for voting
4 equipment and you identified a security
5 vulnerability in that equipment, would you consider
6 that an important thing to -- to fix?

7 A. Yes.

10 THE WITNESS: Sorry.

11 BY MS. KAISER:

12 Q. Your answer was?

13 A. Yes.

14 Q. Thank you.

15 MS. KAISER: All right. Mr. Hamilton, if
16 you'll give us just a minute to confer, I think
17 we're -- we're reaching the end of our
18 questions.

19 THE WITNESS: Okay.

20 MS. KAISER: So we'll go off the record
21 for just a minute, please.

24 (Off the record.)

1 back on the record.

2 BY MS. KAISER:

3 Q. Just a few more questions for you,

4 Mr. Hamilton.

5 Q. Are you aware that Dr. -- Dr. Halderman
6 got access to Fulton County's voting equipment in
7 August of 2020?

8 A. No, I didn't.

9 Q. Okay. You were chief information security
10 officer at the time, August 2020; correct?

11 A. Yes.

12 Q. All right. And were you aware that
13 Dr. Halderman testified in an evidentiary hearing in
14 September of 2020 about that election -- about
15 vulnerabilities in that equipment?

16 A. Was that the same one that I did my
17 testifying in or is that a different one?

18 Q. I'm sorry. Did you ever testify at a
19 hearing?

20 A. Yes, ma'am. I was -- I had, like, two
21 questions asked of me, but yeah. It was a
22 federal -- I thought it was the Curling case, the
23 initial part of it, with Judge Totenberg. She asked
24 me to clarify a couple of terms. But --

25 Q. Okay.

1 A. -- that was when -- that was when we -- we
2 got Zoom bombed that day. Do you recall that?

3 Q. You know, I wasn't present at the hearing,
4 so I can't recall.

5 A. Okay.

6 MS. KAISER: And, Carey, I'm not sure if
7 you recall either if that was the
8 September 2020 hearing.

9 MR. MILLER: My understanding of the
10 question, I think so, yeah.

11 MS. KAISER: Okay.

12 BY MS. KAISER:

13 Q. Well, so did -- were you present for
14 Dr. Halderman's testimony --

15 A. No.

16 Q. -- in a -- in a hearing?

17 A. No, no, no. I only -- the only people I
18 saw were the ones that were on that day, and he was,
19 I think, on a previous day. That's why I had to
20 respond in writing for his stuff.

21 Q. And are you aware -- are you aware that he
22 testified that he was able to hack the election
23 equipment from Fulton County?

24 MR. MILLER: Objection. Lack of
25 foundation. Calls for speculation.

1 THE WITNESS: Yeah, I -- I didn't realize.

2 No, I didn't hear that.

3 BY MS. KAISER:

4 Q. And he was able to do so in just three
5 days?

6 MR. MILLER: Objection. Lack of
7 foundation. Calls for speculation.

8 BY MS. KAISER:

9 Q. You're --

10 A. And this is the --

11 Q. -- not aware of that testimony?

12 A. No. Just as it pertains to that list that
13 I gave.

14 Q. This is not -- this is not about the list
15 of -- from Fortalice; this is --

16 A. Okay.

17 0. -- this is separate.

18 A. Yeah. I wasn't present for any of that.

19 Q. Okay. And you were not made aware of
20 Dr. Halderman's testimony regarding hacking the
21 actual election equipment from Fulton County?

22 A. No, I was not.

23 MR. MILLER: Objection. Asked and
24 answered.

25 THE WITNESS: Sorry.

1 BY MS. KAISER:

2 Q. Would you expect to be made aware of
3 that -- of testimony that the election equipment
4 that Georgia had and was using was able to be hacked
5 in three days?

6 MR. MILLER: Objection. Calls for
7 speculation.

8 THE WITNESS: Yeah, I would think so.

9 BY MS. KAISER:

10 Q. And as -- in your role as chief
11 information security officer for the Secretary of
12 State's office, that's something that you would have
13 liked to know about; is that right?

14 MR. MILLER: Objection. Calls for
15 speculation.

16 COURT REPORTER: The answer again, please?

17 BY MS. KAISER:

18 Q. But nobody told you about that testimony
19 from Dr. Halderman?

20 MR. MILLER: Objection. Lack of
21 foundation. Asked and answered.

22 COURT REPORTER: I didn't hear the
23 previous answer to the question -- the previous
24 question.

25 THE WITNESS: No. "No" was on both.

1 Yeah.

2 COURT REPORTER: Thank you.

3 MS. KAISER: I just want to make sure,
4 Ms. Barnes -- I'm sorry, I don't have access to
5 the realtime -- which question did you not have
6 an answer to?

7 COURT REPORTER: One moment, please.

8 (Whereupon, the record was read by the
9 reporter as follows:

10 Question, "In your role as chief
11 information security officer for the Secretary
12 of State's office, that's something that you
13 would have liked to know about; is that
14 right?")

15 THE WITNESS: And I said, yes, that would
16 be nice to know.

17 BY MS. KAISER:

18 Q. Do you have any idea why nobody told you
19 about this testimony from Dr. Halderman?

20 MR. MILLER: Objection. Calls for
21 speculation.

22 THE WITNESS: I don't.

23 BY MS. KAISER:

24 Q. Are you aware of any measures to mitigate
25 the hack that Dr. Halderman executed on the Fulton

1 County election equipment?

2 A. No, I --

3 MR. MILLER: Objection. Lack of
4 foundation. Calls for speculation.

5 THE WITNESS: No, I -- I would expect that
6 to be a Dominion thing. So...

7 BY MS. KAISER:

8 Q. You think -- do you think the Georgia
9 Secretary of State's office would be involved,
10 though?

11 MR. MILLER: Objection. Calls for
12 speculation.

13 THE WITNESS: I -- I would think as a
14 customer, yeah.

15 BY MS. KAISER:

16 Q. And who within the -- the Georgia
17 Secretary of State's office would have
18 responsibility over that?

19 A. Over the machines themselves?

20 Q. Yes, or -- yeah, over identifying or
21 mitigating vulnerabilities with the machines
22 themselves.

23 MR. MILLER: Objection. Lack of
24 foundation.

25 THE WITNESS: Yeah, it was my

1 understanding that all of them are actually
2 owned by the individual counties. So --

3 But, yeah, I still think the Secretary of
4 State would want to know that information and
5 then do -- you know, get somebody excited about
6 fixing it if that was the case.

7 BY MS. KAISER:

8 Q. And the person within the Secretary of
9 State's office under whose purview that would fall,
10 don't you think that would be the chief information
11 security officer?

12 MR. MILLER: Objection. Calls for
13 speculation. Lack of foundation.

14 THE WITNESS: I guess if it was in scope,
15 probably, yep.

16 BY MS. KAISER:

17 Q. So this shouldn't just be a Dominion
18 thing, as you said earlier; right? That's something
19 that --

20 A. Well, I mean, it's their -- it's their
21 equipment and it's their code line, so, you know, we
22 can't fix it for them. They would have to do it for
23 us, much like PCC would have to fix their software
24 for us.

25 Q. But the Secretary of State's office would

1 have a great interest in making sure that those
2 vulnerabilities were fixed; correct?

3 A. I would think --

4 MR. MILLER: Objection --

5 THE WITNESS: -- so.

6 MR. MILLER: -- asked and answered. Calls
7 for speculation.

8 MS. KAISER: Did you get that answer,
9 Ms. Barnes?

10 COURT REPORTER: I heard, "I would think
11 so."

12 BY MS. KAISER:

13 Q. Are you aware, Mr. Hamilton, that
14 Fortalice conducted an assessment of the BMD
15 equipment in 2019?

16 A. No, actually, not -- you mean the actual
17 polling equipment in the --

18 Q. (Nodded head.)

19 A. No, I didn't realize they did that. That
20 must have been on a -- on a separate statement of
21 work.

22 Q. So you had no involvement with -- with
23 that assessment by Fortalice of the equipment
24 itself?

25 A. No. And it might be just because it was

1 excluded from my statement of work from TrustPoint.
2 You know, it was specifically excluded that the
3 actual voting tabulating, Dominion or whatever, was
4 excluded from my responsibilities.

5 MS. KAISER: All right. Just one -- one
6 more minute, Mr. Hamilton. Thank you.

7 THE WITNESS: Okie doke.

10 MS. KAISER: [Inaudible], please.

11 | VIDEOGRAPHER: I'm sorry. You broke up.

12 MS. KAISER: I said go off the record,
13 please.

16 (Off the record.)

19 BY MS. KAISER:

20 Q. Mr. Hamilton, just -- I just want to make
21 sure the record is clear.

22 You're not aware of any request by anyone
23 from the Secretary of State's office to Dominion to
24 fix any of the vulnerabilities that Dr. Halderman
25 identified with the Fulton County voting equipment;

1 is that correct?

2 A. That is --

3 MR. MILLER: Objection --

4 THE WITNESS: -- correct.

5 MR. MILLER: -- lack of foundation.

6 THE WITNESS: I -- I don't recall any
7 conversation specific to Fulton County except
8 for that notebook we talked about.

9 BY MS. KAISER:

10 Q. That was a laptop.

11 A. Laptop, yeah, notebook. Sorry.

12 Q. Right.

13 So with respect to the Fulton County
14 voting equipment that Dr. Halderman tested and was
15 able to hack, you don't recall any instruction to
16 Dominion to fix anything related to that?

17 A. No.

18 MR. MILLER: Objection. Lack of
19 foundation. Asked and answered.

20 THE WITNESS: No.

21 MS. KAISER: All right. No further
22 questions from me, Mr. Hamilton. Thank you
23 very much for your time today.

24 THE WITNESS: Thank you.

25 MR. MILLER: Dave, I'm going to have a

1 you never worked on the ballot-marking devices
2 themselves?

3 A. No, sir, not in any --

4 Q. Never worked on the printer?

5 A. Nope.

6 Q. Never worked on the scanner into which the
7 ballots were fed?

8 A. No, sir.

9 Q. Okay. And was that type of work beyond
10 your work scope?

11 A. It was.

12 Q. So Ms. Kaiser asked you a couple of
13 questions concerning Dr. Halderman.

14 Do you recall that?

15 A. Yes.

16 Q. Are you aware that the report he worked on
17 concerned hacking of that same voting equipment?

18 A. I -- I didn't correlate the two, no.

19 Q. Okay. Knowing that, that would then be
20 outside of your work scope; right?

21 A. Yes.

22 Q. You talked earlier with Ms. Kaiser about
23 the EMS system.

24 Do you recall that?

25 A. Uh-huh.

Page 207

1 C E R T I F I C A T E
2
3

4 STATE OF GEORGIA:
5
6

7 COUNTY OF FULTON:
8
9

10 I hereby certify that the foregoing transcript was
11 taken down, as stated in the caption, and the
12 questions and answers thereto were reduced to
13 typewriting under my direction; that the foregoing
14 pages represent a true, complete, and correct
15 transcript of the evidence given upon said hearing,
16 and I further certify that I am not of kin or
counsel to the parties in the case; am not in the
regular employ of counsel for any of said parties;
nor am I in anywise interested in the result of said
case.

17
18
19
20
21
22
23
24
25
Lee Ann Barnes

LEE ANN BARNES, CCR B-1852, RPR, CRR, CRC

COURT REPORTER DISCLOSURE

Pursuant to Article 10.B. of the Rules and Regulations of the Board of Court Reporting of the Judicial Council of Georgia which states: "Each court reporter shall tender a disclosure form at the time of the taking of the deposition stating the arrangements made for the reporting services of the certified court reporter, by the certified court reporter, the court reporter's employer, or the referral source for the deposition, with any party to the litigation, counsel to the parties or other entity. Such form shall be attached to the deposition transcript," I make the following disclosure:

I am a Georgia Certified Court Reporter. I am here as a representative of Veritext Legal Solutions. Veritext Legal Solutions was contacted to provide court reporting services for the deposition. Veritext Legal Solutions will not be taking this deposition under any contract that is prohibited by O.C.G.A. 9-11-28 (c).

Veritext Legal Solutions has no contract/agreement to provide reporting services with any party to the case, any counsel in the case, or any reporter or reporting agency from whom a referral might have been made to cover this deposition. Veritext Legal Solutions will charge its usual and customary rates to all parties in the case, and a financial discount will not be given to any party to this litigation.

Lee Ann Barnes

LEE ANN BARNES, CCR B-1852B, RPR, CRR, CRC